Remote Access - Verify II Central Directory

This chapter covers the following topics:

- Description

- Procedure

- Batch Example

Description

Program

B74052

Function

Verify remote access authorization records in the central directory's authorization tables against the Con-nect system file. If a discrepancy occurs, data in the Con-nect system file are assumed to be correct and the central directory's authorization tables are updated.

If you want to display the discrepancies between the central directory's authorization tables and the Con-nect system file, mark both fields. In this case, the records are not modified.

Online Input Screen

```
 11:20 AM              * * *  C O N - N E C T  3  * * *              14.Feb.94
 Cabinet LS                   Remote Cabinet Access                     B74052

                         Recover Directory File

                 Mark _ with any character
                        to start recover procedure
                        for node Node-Name

                 Mark _ with any character
                        to run this function
                        with mode = 'report-only'




 Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
           Menu  Quit
 Complete the information above and press ENTER to continue
```

Utility Parameters

Parameter	Format	Description
Start Recover	A1	
Report Only	A1	

Procedure

This utility verifies and modifies only the records applicable to your Con-nect node.

Processing Sequence

When this utility is run, the following steps are performed:

1. **Check table of users - Con-nect**
   All users authorized in the Con-nect system file are verified against the central directory's authorization tables. If a user is not authorized in the authorization tables, authorization for the user is restored.

2. **Check table of users - Central Directory**
   All authorized users in the central directory's authorization tables are verified against the Con-nect system file. If a user is not authorized or defined in Con-nect, authorization for that user is deleted from the authorization tables.

3. **Check table of cabinets - Con-nect**
   All authorized public cabinets in the Con-nect system file are verified against the central directory's authorization tables. If a cabinet is not authorized in the authorization tables, authorization for the cabinet is restored.

4. **Check table of cabinets - Central Directory**
   All authorized public cabinets in the central directory's authorization tables are verified against Con-nect. If a cabinet is not authorized or defined in Con-nect, authorization for that cabinet is deleted from the authorization tables.

5. **Check table of members - Con-nect**
   All authorized external memberships in the Con-nect system file are verified against the central directory's authorization tables. The following occurs:

   - If an external membership is not authorized in the authorization tables and the external user is not authorized by his local Con-nect, authorization for the membership is deleted from Con-nect.

   - If an external membership is not authorized in the authorization tables but the external user is authorized by his local Con-nect, authorization for the membership is restored in the authorization tables.

6. **Check table of members - Central Directory**
   All authorized external memberships in the central directory's authorization tables are verified against the Con-nect system file. If an external membership is not authorized in Con-nect, authorization is deleted from the authorization tables.

Batch Example

Verify remote access authorization records in the central directory's authorization tables against the Con-nect system file. If a discrepancy occurs, data in the Con-nect system file are assumed to be correct and the authorization table is to be updated. This would be coded as follows:

```
LOGON SYSCNT2B
MENU
B74052 X,
FIN
```